Amendments to the Specification:

Please replace the paragraph beginning at page 9, line 4 with the following amended paragraph:

If the connection constraints are not satisfied (step 453), then the secured service 170 may not accept the authorization information and may refuse the connection. Upon refusal of the connection by the secured service 170, the client 110 may determine whether it is appropriate to retry connecting using the authorization information (step 460). For instance, it may be appropriate to retry where the authorization information has been refused less than a predetermined number of times and/or where the connection constraints associated with the authorization information are not known to be violated. If determined appropriate, the client 110 may again provide the authorization information to the secured service 170 (step 451). Otherwise, the client 110 may or may not receive a report of the failed connection ~~(step 470)~~ and/or request that the broker service 150 broker a connection with another secured service 170 (step 413).

Please replace the paragraph beginning at page 12, line 1 with the following amended paragraph:

Fig. 8 illustrates a process for establishing a connection to the secured system by presenting the constrained password to the secured system that may be used in one implementation of the process 450 of Fig. 4. The client 110 may present the constrained password to the secured service 170 at the connection point (step 805) and the secured service 170 may receive the constrained password at the connection point (step 810). Thereafter, the secured service 170 may determine if the constrained password satisfies the connection constraints, such as, for example, a constraint that the constrained password match the constrained password previously stored, that the constrained password has not previously been presented and/or used (e.g., the constrained password may be a one-time use password), that the constrained password is presented within an acceptable time window (e.g., the constrained

password may be a time limited password) (step 810). The secured service 170 may refuse the connection if the constrained password does not satisfy the connection constraints, and the client 110 then may execute a retry procedure (step 815) that may correspond generally to step 460 of the process of Fig. 4. Otherwise, if the constrained password does satisfy the connection constraints (step 810), then the secured service 170 may allow the connection to be established (step 820).